Department of Defense

Information Management (IM) Strategic Plan

Information Superiority

Version 2.0

Department of Defense
Chief Information Officer

October 1999

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 1999		**00-00-1999 to 00-00-1999**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Management (IM) Strategic Plan	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense,Chief information Office,Washington,DC,20301-1000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**42**	

Link to signed Foreword (.pdf)

Foreword

The initial Information Technology Management (ITM) Strategic Plan published in March 1997 was a trailblazing effort. This was due to the support from the entire Department of Defense (DoD) information technology (IT) community. Continued participation will ensure that this becomes a useful living document that evolves to chart our course for using IT in DoD. This plan has been retitled the DoD Information Management (IM) Strategic Plan, to better reflect the Department's focus on overall management of information, not just management of IT. This plan provides overall DoD guidance for managing information resources and establishes the DoD vision for IM, top goals and objectives, and strategies for accomplishing the goals. This plan supports the DoD corporate-level goals, the *Report of the Quadrennial Defense Review (QDR)*, the *Defense Reform Initiative Report (DRIR*), and *Joint Vision 2010 (JV2010).*

Subdivision E of the Clinger-Cohen Act (CCA) of 1996 (formerly the Information Technology Management Reform Act of 1996) mandates that we improve our day-to-day mission processes and properly use IT to support those improvements. Technology must be fielded orderly, promptly, and efficiently. We must use streamlined acquisition processes, commercial off-the-shelf (COTS) products and services, outsourcing, and partnering, as appropriate, to take advantage of industry capabilities. The IT investment portfolio concept, as put forth in CCA, emphasizes the need to do a better job of prioritizing IT capital investments and being accountable for results. Accountability extends from the individual to the mission commanders and Congress. Keeping our military and civilian workforce trained in new technologies and improved processes is critical to maintaining our fighting edge and achieving savings. Finally, all this is in vain if our information is not protected.

It is our job to implement management processes that streamline development and acquisition programs, to be mindful of costs, and to provide the best support to DoD's mission that we possibly can. We need to continue to work to find better ways of bringing available information services and technologies into our warfighting, operational and support missions. We are institutionalizing processes reflecting the full spirit and intent of the CCA. Senior management - including civilian, military and political appointees - understands implementation will take time, but we must proceed without hesitation.

All of us need to change the way we do our jobs and improve mission accomplishment, fully exploiting IT. We must effectively integrate DoD's IM program requirements with the Joint Staff's evolving *JV2010* Information Superiority concepts, taking a broad view of IM appropriate to the Information Age. As the *JV2010* Information Superiority Coordinating Authority, the Joint Staff is implementing the Global Information Grid (GIG) to provide secure, seamless, flexible information services and technology to the warfighter.

This strategic plan provides a roadmap for pursuing significant improvements well into the next century. However, the execution of this plan requires commitment to work together toward our common goals. It is in this context that DoD Component Chief Information Officers (CIOs) will develop individual plans that support the goals, objectives, strategies, and measures of this plan.

Continued success will require sustained cooperation, accountability, and refinements. Our best efforts depend upon a strong commitment to openness and trust. We have the opportunity to make a difference. I urge your continued support.

DoD Chief Information Officer

Executive Summary

Information has a central role in national defense. The *QDR* highlights many aspects of the use of IT to support our national security strategies. DoD has established two corporate-level goals:

> *"Goal 1. Shape the international environment and respond to the full spectrum of crises by providing appropriately sized, positioned, and mobile forces.*
> *Goal 2. Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure."*

The information revolution is creating the Revolution in Military Affairs (RMA) of Goal 2 that will fundamentally change the way U.S. forces fight. We must use our informational assets and the associated changes in the way we approach warfighting to dominate in battle. Our template for seizing on these technologies and ensuring military dominance is *JV2010*, the vision set forth by the Chairman of the Joint Chiefs of Staff for military operations of the future. At the same time, we must ensure that the defense infrastructure is managed in a manner that is most efficient and effective by eliminating duplication and reducing cost, while maintaining required information support. This is a part of the concomitant Revolution in Business Affairs (RBA) and reengineering of the Department, also part of Goal 2.

JV2010 recognizes information superiority as the foundation for new joint doctrine and concepts as we move towards 2010. As the Information Superiority Coordinating Authority, the Joint Staff's work defined the challenges and capabilities to be resolved to provide the warfighter with the assured knowledge and battlespace visualization required for 2010 operations through the GIG.

> "*Improvements in information and systems integration will … impact future operations by providing decision makers with accurate information in a timely manner and … gain dominant battlefield awareness… We must have information superiority; the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same…"*

We must exploit the RMA and RBA to meet the challenges of an uncertain future and ensure we maintain information superiority over our adversaries. *Information superiority is not only the foundation of new military concepts – it is the key to reinventing the defense infrastructure.*

To meet this responsibility, the Department must have a strategic plan that addresses the management and use of IM capabilities. Thus this DoD IM Strategic Plan provides overall direction and guidance for managing the Department's information resources. It establishes the DoD vision for IM, top goals and objectives, and strategies to accomplish the goals.

The vision statement aligns with *JV2010* and its emphasis on information superiority.

Vision: Information superiority achieved through global, affordable, and timely access to reliable and secure information for worldwide decision-making and operations.

The mission of the IM community is intended to support this vision.

Mission: Provide, in a secure fashion, the right information, at the right place and time from the right sources, in a form that users can understand and reliably use to accomplish their missions and tasks, effectively and efficiently**.**

To help realize the IM vision and mission, Section IV of the DoD IM Strategic Plan describes the strategic direction. Four goals describe areas for major change. Each goal statement is followed by a description to outline the context for the goal. Objectives and strategies characterize broad actions needed to pursue each goal. In general this plan will capitalize on DoD Component programs and projects to accomplish the strategies and on resource reporting aligned with OSD level Planning, Programming, and Budgeting System (PPBS) criteria.

Four goals characterize fundamental DoD critical success factors for IM to realize the vision.

Goal 1, "***Become a mission partner,"*** grounds IM in our national defense mission using joint mission planning and analysis processes as the basis for defining information service and performance requirements.

Goal 2, "***Provide services that satisfy customer information needs**,"* builds on Goal 1 requirements by using the customer/supplier model to meet mission service requirements.

Goal 3, "***Reform IT management processes to increase efficiency and mission contribution,"*** captures the essence of CCA, emphasizing the management process improvements that are needed to more effectively deliver information and services to DoD mission customers.

Goal 4, "***Ensure DoD's vital information resources are secure and protected**,"* reflects the pervasive impact of information assurance on DoD.

This strategic plan provides a roadmap to realize more efficient and effective mission support. The execution of this plan requires leadership and commitment to work toward our common goals. It is in this context that DoD Component CIOs need to develop individual plans that include specific initiatives and actions that reflect a jointness and commonality of purpose and provide a sound foundation for improving processes and ensuring that resources are in the right place to support our mission. This DoD IM Strategic Plan does not address specific programs or budgets. It serves as a framework for the development of more detailed DoD Component plans that identify specific programs and initiatives and relate them back to the overall DoD mission.

This strategic plan complies with the CCA and the Government Performance and Results Act (GPRA), Paperwork Reduction Act (PRA), and other Office of Management and Budget (OMB) mandates and guidelines. This body of laws and regulations has provided the opportunity to move from budget and acquisition centric decision making to mission, architecture, service and performance decision making.

The DoD CIO is the agency executive responsible for ensuring that the CCA mandate is executed within the full spirit and intent of the law. The extensive experience and talent of DoD IM support personnel, the emerging private information capabilities, and strong Congressional guidance provide a wealth of new opportunities for improvement.

Table of Contents

Appendices

I. Introduction

A. Purpose

The DoD IM Strategic Plan provides overall DoD guidance for managing its information resources. The plan establishes the DoD vision for IM, top goals and objectives, and strategies to accomplish the goals. The plan:

- Links IM to joint warrior operational needs and mission support needs.
- Provides the long-term direction for IM planning.
- Helps coordinate and integrate IM activities horizontally across functional areas and organizations and vertically between the DoD Components.
- Creates mechanisms to systematically manage and direct DoD IM resources and programs.
- Complies with provisions of the CCA.

The plan fulfills the strategic planning requirements of the PRA of 1995, as amended, and OMB Circular A-130.

B. Scope

The DoD IM Strategic Plan pertains to information management, information technology, information resources management, information systems, and information services activities across the DoD. It applies to all organizations in the Department, including the Office of the Secretary of Defense, the Joint Staff, the Unified Commands, and the DoD Components. In this plan the term "DoD Components" will be used to represent Military Departments and Defense Agencies and activities as a group. The plan will apply to interfaces between the Department and external organizations including other Government agencies, the private sector, non-profit organizations, allies, coalition partners, the North Atlantic Treaty Organization (NATO), and other alliances. The scope includes all DoD information technology, including national security systems (NSS), as defined in the CCA. It applies to all DoD activities that provide or use information, and oversee, plan, resource, develop/acquire, or operate information capabilities for the warfighter and those who support the warfighter.

C. Relationships to Other DoD Policy and Guidance

DoD policy requires integrated IT strategic planning for DoD. The Under Secretary of Defense Comptroller (USD(C)) memorandum of October 16, 1997, states that this IM plan must link to the DoD Strategic Plan. Additionally, it states that subordinate level strategic planning documents will link hierarchically to the DoD IM Strategic Plan. The DoD IM Strategic Plan addresses improvements to management processes affecting DoD-wide strategic planning, requirements generation, programming and budgeting, and operations. In accordance with section 5122 of the CCA, the IM Strategic Plan is also the IT link for the PPBS, between the Defense Planning Guidance (DPG) and the Program Objective Memorandum (POM).

D. Strategic Plan Structure

This DoD IM Strategic Plan serves as a framework for the development of more detailed DoD Component plans that identify specific programs and initiatives, and relate them back to the overall DoD mission. It outlines the priority information and IT initiatives and facilitates the identification of common efforts and overlapping missions. These will be reviewed during planning and budget processes both at the DoD Component level and at OSD. The plan complies with the CCA, GPRA, PRA, and other OMB mandates and guidelines.

Section I provides the purpose, scope, and structure.

Section II describes the National and Defense Strategies that this plan supports.

Section III describes the vision of the future for information management.

Section IV describes the mission and strategic direction for the 21st century. Goals describe areas of major change to realize the vision. A description and conceptual diagram outline the context for the goals. Objectives and strategies characterize broad actions to pursue each goal. In general, DoD Component programs and projects will support and accomplish the strategies. The plan will be a framework for integrating all IM activities across DoD into a coherent and comprehensive program. Future versions of the plan will continue to extend and tailor IM guidance to the broad set of DoD IM activities that lie outside the traditional information resources management (IRM) and automated information system (AIS) domains. The relationships and dependencies of key information initiatives such as *JV2010* information superiority implementation; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) modernization; DoD modeling and simulation (M&S); and weapons systems IT environments, mission support systems and infrastructure modernization will be identified.

Section V addresses the implementation of this plan, both within the framework of the DoD PPBS and specific actions to be taken by the CIO community.

Appendix A provides IM Guiding Principles. Appendix B describes the IM strategic planning process and shows the links of the IM Plans with DoD and functional strategic plans, and with the PPBS process. It also defines the update cycle for this strategic plan and describes how this plan interfaces with the DoD PPBS through the DPG and POM. Appendix C describes the IT Performance Measurement Strategy and Implementation Program. A list of acronyms is provided at Appendix D. A glossary of major terms is provided at Appendix E.

The plan does not address specific programs or budgets. A common vision and strategic direction must first guide implementation activities. The Department cannot achieve *JV2010* or its top goals if it does not have a common strategy. Each Component will develop its portfolio of information technology investments, based on identified criteria, to accomplish DoD goals, objectives and strategies.

E. Reference Links

The link to the CCA, PRA, GPRA, and other pertinent CIO documents is located at http://www.c3i.osd.mil/org/cio/index.html.

The link to DoD publications such as the *National Security Strategy*, *QDR*, *DRIR*, and *JV2010* is located at http://www.defenselink.mil/pubs.

The link to Component CIO sites and their supporting IM strategic plans is located at http://www.c3i.osd.mil/org/cio/dodcios.html.

II. National and Defense Strategies

Our national security strategy revolves around our long-standing goals as a nation to maintain the sovereignty, political freedom, and independence of the United States, with its values, institutions, and territory intact; to protect the lives and personal safety of Americans, both at home and abroad; and to provide for the well-being and prosperity of the nation and its people.

In order to support this national security strategy, the U.S. military and the Department of Defense must be able to help shape the international security environment in ways favorable to U.S. interests, respond to the full spectrum of crises when directed, and prepare now to meet the challenges of an uncertain future. These three elements - shaping, responding, and preparing - define the essence of U.S. defense strategy between now and 2015. The *QDR* highlights this strategy.

DoD has established two corporate-level goals:

> *"Goal 1. Shape the international environment and respond to the full spectrum of crises by providing appropriately sized, positioned, and mobile forces.*
> *Goal 2. Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure."*

The information revolution is creating the RMA of Goal 2 that will fundamentally change the way U.S. forces fight. We must exploit these and other technologies to dominate in battle. Our template for seizing these technologies and ensuring military dominance is *JV2010*, the vision set forth by the Chairman of the Joint Chiefs of Staff for military operations of the future. At the same time, we must ensure that the defense infrastructure is managed in a manner that is most efficient and effective by eliminating duplication and reducing cost, while maintaining required information support. This is a part of the concomitant Revolution in Business Affairs (RBA), Revolution in Military Logistics (RML) and reengineering of the Department, also part of Goal 2.

JV2010 recognizes information superiority as the foundation for new joint doctrine and concepts as we move towards 2010.

> "*Improvements in information and systems integration will … impact future operations by providing decision makers with accurate information in a timely manner and … gain dominant battlefield awareness… We must have information superiority; the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same…"*

We must exploit the RMA and RBA to meet the challenges of an uncertain future and ensure we maintain information superiority over our adversaries. *Information superiority is not only the foundation of new military concepts – it is the key to reinventing the defense infrastructure*. The Information Superiority Coordinating Authority in the Joint Staff is implementing the GIG to provide this defense infrastructure.

Exploiting the "Revolution in Military Affairs"

For several years, the U.S. military and DoD have been engaged in a variety of efforts to exploit the RMA. *JV2010* articulates the Chairman's vision of a 21st century military in which information

superiority is the key to achieving full spectrum dominance through the synergy of four new operational concepts: dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. Achieving full spectrum dominance requires continuing evolution to an integrated "system of systems", whose core is a C4ISR architecture. The Joint Staff's GIG concept advances the DoD beyond the current Defense Information Infrastructure (DII) to an Information Superiority capability fused with weapon systems to enable Full Spectrum Dominance for *JV2010* and beyond. The GIG envisions a baseline capability integrating all DoD C4ISR requirements – strategic, operational, tactical, and base/post/camp/station/ship – providing flexible, assured bandwidth to warfighters regardless of environment. The GIG will create that integrated "system of systems" through its Capstone Requirements Document (CRD). The GIG CRD will provide the framework to tie disparate DII programs into a seamless foundation to support warfighter's IT requirements.

In warfare, the information superiority that these capabilities provide will "lift the fog of war", significantly increase the speed of command-level decisions, enable forces to take the initiative away from adversaries, and set the conditions for early, favorable termination of any conflict.

Exploiting the "Revolution in Business Affairs"

A Revolution in Business Affairs also has begun. Efforts to reengineer and streamline the Department's infrastructure and business practices must parallel the work being done to exploit the Revolution in Military Affairs if we are to afford both adequate investments for the future, especially a more robust modernization program, and capabilities sufficient to support an ambitious shaping and preparation strategy throughout the period covered by the *QDR*. This thrust was reinforced by the report of the *DRIR*, which stresses the use of IT to improve Departmental performance. Chapter One of this report places emphasis on moving towards electronic business operations (EBO) in the Department across all functional areas and not just procurement and payment. In support of the *DRIR* and Access America, the CIO has released a DoD Electronic Business/Electronic Commerce (EB/EC) Strategic Plan, which provides the DoD with an EB/EC vision and associated goals, objectives and strategies. This plan is located at http://www.c3i.osd.mil/org/cio/index.html.

The concept of focused logistics requires a far more agile and responsive infrastructure so the U.S. can rapidly project power abroad, and its forces can "reach back" to their home base for vital support. New threats make securing our critical information resources wherever they are located essential to our security.

Creating a DoD Enterprise Architecture and Common IT Infrastructure

With the support of an advanced architecture that relies on a seamless information technology infrastructure, the United States will be able to respond rapidly to any conflict. This architecture will enable warfighters to dominate any situation and day-to-day operations will be optimized with accurate, timely, and secure information. The GIG provides the vision and means to implement the IT infrastructure required for the warfighter's battlespace visualization and decision-making process.

Just as much oasthe non-defense world has become increasingly interconnected through the growth of global and national networks, the DoD is working to provide a complementary, secure, open GIG with a globally connected, networked infrastructure. The GIG will provide this seamlessly integrated capability to support all functional missions and reach from the home base to the front-line. It will link as one team with one purpose; our forces and support organizations, other agencies, industry, our allies and coalition partners. New technology harnessing the power of information gives us the ability to transform our defense to meet the emerging threats and challenges of the 21st century.

III. Vision of the Future

The overarching vision statement aligns IM with *JV2010* and its emphasis on information superiority.

Vision

Information superiority achieved through global, affordable, and timely access to reliable and secure information for worldwide decision-making and operations.

To fully understand this vision, we must imagine that it is 2010 or beyond. The Department has applied the guiding principles contained in Appendix A. The DoD IM Strategic Plan has been implemented. What will that world look like for defense? How will information be used in the future DoD?

DoD has been and will continue to be an IM leader. We will be at the forefront of new technology, either as the creator, developer, or user. Our commanders, researchers, teachers, and support contractors fervently pursue new technologies to maintain our military superiority. Congress and the American people recognize the importance of these initiatives and will provide the required resources to maintain that technological leadership. Commercial IT innovation will enable military applications.

In 2010 and beyond, IM is the foundation of mission effectiveness. Information management is integral to our command and control, intelligence, and mission support functions. Computers are a normal part of the work environment from office to warehouse. While Components may be at different levels of IT, there will be a seamless integration of information flow implemented through the GIG IT infrastructure.

Global Information Grid (GIG)

The Department operates a secure GIG that enables electronic government and achieves Information Superiority. The GIG's IT infrastructure depends upon its CRD to integrate the DII's disparate programs. The GIG provides a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

Command and Control (C2)

The "fog of war" has been substantially lifted through our intelligence, surveillance and reconnaissance (ISR) capabilities. A common operating picture lets joint commanders see the three-dimensional battle space in near-real time. Our C2 systems develop courses of action and executable plans in minutes, after simulation and analysis of all options. C2 systems seamlessly link the national, theater, operational and tactical levels, to ensure vertical and horizontal integration of forces. Where reaction times must be in seconds, sensors acquire targets and pass that information directly to smart weapons over high bandwidth communications pipes. The pace at which we operate paralyzes our adversaries. We use information warfare against our enemies, while protecting our own vital information resources. U.S. systems are interoperable with allied and coalition systems and DoD partnerships with other government agencies are enabled by interoperable and integrated systems and infrastructure. Information superiority is the basis of U.S. full spectrum dominance.

Intelligence

The intelligence community is an agile enterprise. Information from the best sources flows into multi-disciplined, cross-organizational teams of analysts that respond quickly and effectively to continuing threats and immediate crises. An astonishing volume of information is gathered through all source collection methods, is assessed, and in many cases is further enriched to assure its relevance to national policy issues, mission planning, and operational use. For example, ubiquitous sensors scan potential trouble spots continually, night and day, in all weather. Full-spectrum data is focused and filtered so that it can be efficiently processed by teams of production analysts. Data is fed into models and simulations so that options can be realistically assessed. Information can easily flow across security levels. Our information security capabilities ensure the protection of sensitive materiel and sources.

Mission Support

DoD business functions, such as logistics, finance, health, and personnel, are as effective and efficient as similar functions performed in the private sector. Advanced information technology lets us exploit the RBA. Scarce resources are no longer wasted on unnecessary infrastructure and unique applications, and support functions multiply the effects of the RMA. For example, the Department, through the application of EB/EC principles, is virtually paperless. These EB/EC principles are being used to streamline functional processes and conduct all of its business internally and with its suppliers. Smart cards speed purchases and help streamline procurements. Logistic supply systems fill requests for supplies in hours. Asset visibility is maintained at every point of the supply chain (using advanced technologies such as bar coding and scanners), so commanders know where their human and materiel assets are located and when they will be delivered. Standard interfaces, shared data, and the use of commercial standards facilitate outsourcing of activities where appropriate. People routinely telecommute, saving office space and reducing impacts on the environment. Our critical DoD and national information resources are protected against malicious or unintentional harm. By 2010, an enterprise-wide electronic environment will exist where best practices and enabling technologies are used to facilitate the most efficient exchange of the full range of business information resulting in streamlined and rapid response to the warfighter and supporting Defense missions. This vision assumes continued application and emulation of best business practices, as well as continued employment of the best enabling technologies across the DoD EB/EC business environment. It concludes that such applications will streamline and increase the speed of response in accomplishing DoD mission, foremost of which is support to the warfighter.

The new mission capabilities are sustained by new management practices, principles, and processes. Management principles and practices proved by industry and the National Performance Review are now applied across DoD's functional areas and organizational activities. DoD manages its activities through an integrated set of strategic visions, goals and measures grounded in the *QDR, JV2010,*

and other key leadership guidance. IM strategic plans and IT investment portfolios are aligned with functional strategic plans so that the contribution of IM to the mission is clear and compelling. And:

- Processes are benchmarked, eliminated, outsourced, consolidated, standardized and reengineered in accordance with strategic plans before investing in IT.
- Mission analyses and assessments that apply business process reengineering identify better ways to accomplish tasks and meet performance targets.
- Investments in IT are measured with outcome based performance measures that are tied to the business processes the IT investment supports.
- Operational architectures provide a uniform, systematic way to specify needs.
- Solutions integrate information and technology with improvements in doctrine, processes, organizations, training, weapons and other elements of military capability.
- Individual systems and other IT acquisitions are managed in the context of investment portfolios and system of systems architectures.
- IT solutions seamlessly support garrison and deployed modes of operation, reducing training and infrastructure resources.
- The appropriate level of information security is applied, commensurate with risk.

To support its customers as they improve mission performance, the IM community reengineers its internal processes to be more effective and efficient, and changes its culture:

- The IM community has a customer focus and measures customer satisfaction.
- Systems and technical architectures are applied to ensure interoperability and integration.
- The IT acquisition process uses prototypes, demonstrations, and exercises to evolve IT capabilities in full collaboration with end users.
- IT services and products are benchmarked to achieve " world-class" performance at the lowest possible cost.
- IM organizations continually improve their internal processes, such as software design and technology insertion.
- IM empowers its people and embodies the principles of a "learning organization".

The IM community, working in partnership with its customers, has redesigned how it does its business. Culture, organization, training, and processes have been reinvented. Organizations are streamlined to eliminate unnecessary headquarters staff. Individuals are empowered and accountable. Vertical stovepipes and hierarchical thinking has given way to horizontal teaming and cross-functional integration.

New paradigms for IM fully realize the value of information as a resource. Information is managed by and for users. Information specialists help users to find the information they need, assess and assure its fitness for use, and provide professional knowledge as needed through the DII to assure customer satisfaction. The GIG is now seamlessly integrated and transparent to users. New capabilities are continually transitioned into the infrastructure without any disruption in ongoing operations. Advanced technologies such as data mining, intelligent agents, and mobile computing are available to all users regardless of their location or activity.

The *QDR, JV2010* and other DoD strategic plans have established the importance of information to the Department. The extensive experience and talent of DoD IM professionals, IT support personnel, the emerging private information capabilities, and strong congressional guidance provide a wealth of new opportunities for improvement. The goals, objectives and strategies in this plan move the Department in the direction of this vision for the future. IM measures of performance are being designed to help managers assess how much progress we are making.

IV. DoD IM Strategic Direction for the 21st Century

The mission and vision for information management (IM) have a strong link to supporting national defense. The mission statement is derived from the C4ISR Integration Task Force Report of November 1996.

Mission

Provide, in a secure fashion, the right information, at the right place and time from the right sources, in a form that users can understand and reliably use to accomplish their missions and tasks, effectively and efficiently.

Four goals characterize fundamental DoD critical success factors for IM to realize the vision. Goal 1 grounds IM in our national defense mission using joint mission planning and analysis processes as the basis for defining information service and performance requirements. Goal 2 responds to management direction and mission requirements by delivering quality, affordable products and services to IM/IT customers. Goal 3 emphasizes the management process improvements that are needed to more effectively deliver information and services to DoD mission customers. Goal 4 reflects the pervasive impact of information assurance on DoD. The strategies associated with the goals are organized logically but are intended to be implemented in parallel to make rapid progress toward the goals. Figure 1 shows key relationships among the goals.

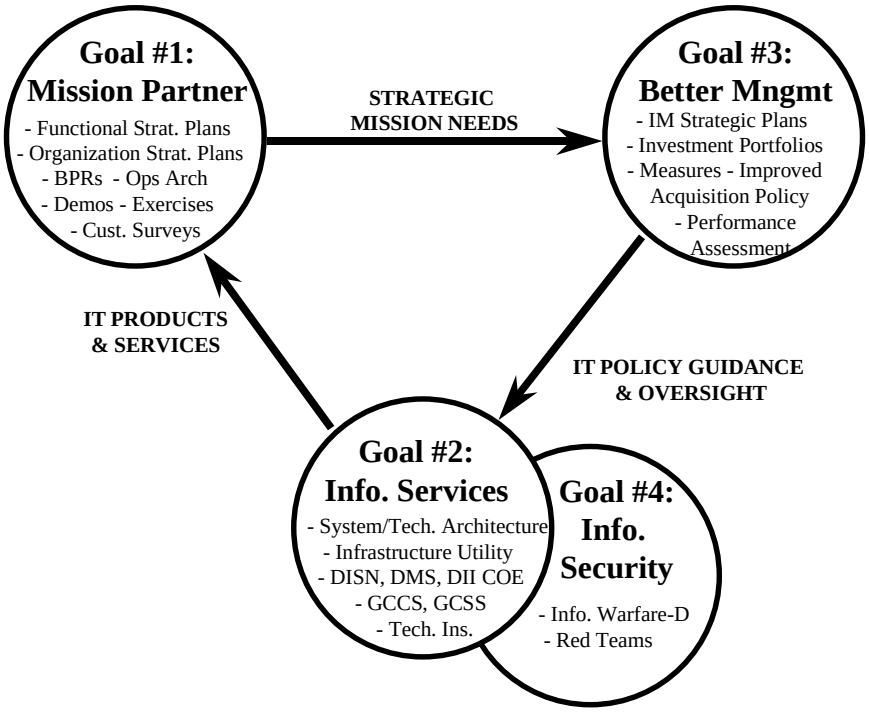
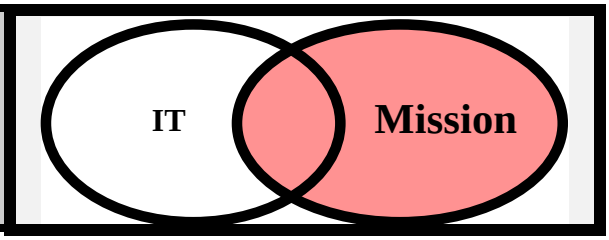


Figure 1. Key Relationships Between the IM Goals

GOAL 1 ***Become a Mission Partner***	

Description: *JV2010* recognizes information superiority as the enabler for full spectrum dominance in the 21st century. The *QDR* extends this vision to business affairs that encompass support missions and the defense infrastructure. Overall, DoD must leverage information resources and technology to improve the performance of missions while realizing major efficiencies in how the Department conducts its business functions. Mission processes, information uses and services must be clearly understood and communicated to drive IT planning and resource decisions. The link from doctrine, strategy, goals, measures, and architectures to IT must be clear and compelling. DoD can use CCA's "focus IT on the mission" direction to address technical and managerial inhibitors to realize the full benefits of IT.

Objective 1.1 - Identify Mission Needs and Align IT

Strategy 1.1.1 - *Influence strategic planning and align IT strategically to mission plans*. Promote strategic planning as the basis for investing in IT. Strengthen collaborative relationships with military commanders and functional managers to help them formulate strategic plans that capitalize on the potential of IT to revolutionize military and business affairs. This strategy envisions having functional strategic plans and Component strategic plans with goals and performance measures for all DoD functional areas to improve defense planning and as a basis for aligning IT with the mission.

Strategy 1.1.2 - *Promote and institutionalize methods to improve mission processes.* Major improvements are recognized by using business process reengineering (BPR) disciplines to rigorously analyze mission area processes and relate those to strategic goals and measures of performance for the mission. Order of magnitude improvements are recognized by integrating processes across current stovepipes. The initial target is to get a core set of consistent process models for all functional areas and activities necessary to analyze opportunities and select those with the highest payoff. This strategy requires inserting BPR methods into the Requirements Generation System and establishing policies for conducting BPR consistently across all mission and mission support domains. DoD must have a comprehensive plan for reengineering its functions to meet CCA requirements to reengineer before investing in IT.

Strategy 1.1.3 - *Employ joint requirements generation processes and architecture products to identify IT needs*. Conduct joint mission assessments and analyses in a systematic manner using uniform methods (e.g., linking to the Universal Joint Task List) to identify mission and mission support objectives, measures, architectures, and strategies that leverage IT. This strategy envisions an assessment and analysis process that addresses all elements of military capability holistically from a Joint and Defense-wide perspective leading to capstone requirements documents that apply operational architectures to define tasks and information exchange requirements. This strategy requires linking the *JV2010* information superiority implementation process, the Joint Warfighting Capabilities Assessment (JWCA) process, Principal Staff Assistant (PSA) planning and assessments, and Component processes to provide an integrated set of desired operational IT capabilities and the adequacy of programs and initiatives to meet the IT need.

Strategy 1.1.4 - *Influence and participate in operational exercises and demonstrations*. This strategy envisions the Department evolving to an integrated, Joint and Defense-wide environment and process for assessing options and programs, and bringing new capabilities to the field. Existing Joint and Defense-wide IT environments are expanded to include mission support IT. Joint, Defense-wide, and Component IT environments for concept exploration, experiments, demonstrations, tests, and modeling and

simulation are fully integrated in distributed networks. The DoD CIO Council maintains a Defense-wide plan for IT participation in exercises, demos, advanced concept technology demonstrations (ACTDs), advanced warfighting experiments (AWEs), and other front-end processes and assessment activities. This comprehensive plan helps implement information superiority and other functional area IM thrusts in support of better mission performance across the Department.

Objective 1.2 - Forge Effective Partnership Relationships with Customers

Strategy 1.2.1 - *Promote organization structures for effective partnering.* The ultimate responsibility for managing processes, investing in IT, and assessing the contribution of IT to the mission rests with commanders, process owners and line managers. This strategy requires positioning IT to influence key functional decisions by designing organizational structures to ensure functional and IM responsibilities are effectively executed and aligned at all levels. Existing management structures need to be assessed in the light of GPRA, Chief Financial Officer (CFO), PRA and CCA mandates. This strategy can be accomplished by a comprehensive, top level review of DoD IT management structures by the CIOs.

Strategy 1.2.2 - *Educate customers on IM and communicate the IM mission.* Customers need to have sufficient knowledge of IM as it impacts their mission to make informed decisions about what IT they need. Effective communication must be in the user's language, not in technical jargon. This strategy requires increased emphasis on educating users about IM's potential for improving mission performance, how to effectively work with the IM community, and how to get the most from IT investments.

Strategy 1.2.3 - *Obtain customer feedback at all levels.* Understanding and acting on customer feedback is essential in forging and maintaining effective partnerships. Senior IM leadership must interact with the Commanders in Chief (CINCS), Service and Agency heads to understand and respond to needs and concerns. This strategy must also extend through all levels of the community, with mechanisms in place to survey customer satisfaction and needs. Customer interaction must be a key influence on strategic plans, BPR, and day-to-day service and information delivery.

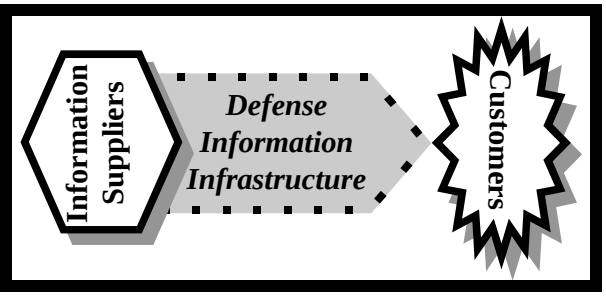
Objective 1.3 - Move Toward an Information Marketplace

Strategy 1.3.1 - *Build a framework to determine the value of information.* Our military capabilities are heavily dependent on focused information. The value of information is a primary discriminator in business decisions and information assurance protection strategies that focus on priority targets. This strategy requires developing and applying knowledge management methods and tools for helping a customer determine the value of information to their missions and tasks (and the risks of not having the information). This methodology, if successful, can help reduce the "glut" of information and enable DoD to treat information itself as a commodity.

Strategy 1.3.2 - *Facilitate flexible access to the best sources of information and services for customers.* The customer should have a full spectrum of interoperable quality information resources and services to choose from, at affordable prices -- a menu of mission/task-related products, services and related cost/performance. The interface to the customer will have many of the characteristics of an information marketplace such as quality/cost comparison information, flexibility, choice of supplier, customer feedback, and ubiquitous help. This strategy envisions new approaches to manage information resources that use market concepts to get customers the products and services on time and at an affordable cost. It envisions increased use of performance contracts, partnering agreements, fee-for-service, and devolution of purchasing of IT to lowest levels.

GOAL 2

Provide services that satisfy customer information needs



Description: To meet its global mission, DoD must focus the information infrastructure on getting information to mission and mission support customers, from multiple information suppliers/providers. The end-state is a seamless, worldwide "infosphere" that allows users anywhere, anytime to "plug" into a Joint, Defense-wide information space. As information generation capabilities become more complex, (e.g., maps, video) DoD must begin to manage the information space for the user and integrate and modernize its information infrastructure. Users need the information services and tools necessary to identify, retrieve, fuse, and format information easily and immediately.

This ubiquitous information capability must support reengineered processes. Better ways of performing military tasks and business functions require advanced technology and powerful new applications. Military operations and command and control functions must be supported by capabilities such as a common operational picture of the battlespace. Initiatives like reengineered travel processes and streamlined procurement are excellent examples of the application of EB/EC principles and processes supported by the proper use of information technology.

The underlying technology platform must be modernized and integrated to support the RMA/RBA. DoD's base-level infrastructure needs urgent attention. A shared data environment to ensure semantic interoperability and cross-functional integration is a priority. A common operating environment throughout DoD, from installations to weapon system platforms, will expedite application system implementation and allow incremental implementation. Infrastructure components must move from an "organization/technology centric" paradigm to an interconnected set of services/products with quantifiable cost and performance measures to determine value-added to the mission. The cost of the infrastructure must be reduced relative to its contribution to the mission.

Management of the end-to-end infrastructure must support the goals of seamless integration and modernization. Today's systems are too often narrowly focused, not fully interoperable, and support a single function or organization requiring users to assemble information from incompatible sources. Breaking out of this stovepipe environment requires new management mechanisms that cross-cut organizational boundaries. Common and shared solutions will reduce unnecessary duplication and cut costs for everyone.

Key to realizing this goal is the GIG. The DII Master Plan identifies the major elements of the information infrastructure, roles and responsibilities, and serves as the tool to track the evolution of the DII into a service environment. The GIG CDR takes the DII programs and major elements and integrates them into a seamless, interoperable "system of systems".

Objective 2.1 - Build An Infrastructure Based on Architectures and Performance

Strategy 2.1.1 - ***Deploy a comprehensive, uniform methodology to define and integrate DoD architectures***. Architectures provide the best, long-term definition of the mission and related IT

support. An integrated architecture framework for operational, systems, and technical architectures must be established to ensure interoperability and consistency. A disciplined support environment, similar to that provided by "data modeling" support tools, would advance a common understanding of missions and IT support by enforcing rigorous element definitions and relationships to other elements. Roles and responsibilities for generating, integrating, and using architectures in managing information and supporting IT must be institutionalized. The Architecture Coordinating Council (ACC) can be a catalyst. The target is a "system of systems" architecture for the GIG that can be expanded to include all missions. Technical architectures should bridge the gaps between weapons, platforms, and information systems. Interoperability must be "built-in" throughout the process, from requirements generation through certification and testing, and demonstrated in "live" environments like the Joint Battle Center (JBC).

Strategy 2.1.2 - *Build performance measures into the infrastructure*. This strategy envisions having performance measures for all GIG products and services. When complete, efficiency and investment decisions can be based on systematic assessments of information cost and value added to mission customers. Fielding a user oriented performance management system to systematically capture, archive, and report performance information is part of this strategy.

Objective 2.2 – Ensure DoD Systems Meet the Year 2000 (Y2K) Challenge

Strategy 2.2.1 - *Fix the Y2K problem.* The objective is to experience no disruption at the turn of the century and have capabilities to respond quickly to residual errors. The Y2K Management Plan is the basis for a coordinated approach across the Department. Experience and tools will be shared and exploited.

Strategy 2.2.2 - *Measure & assess Y2K progress*. Track the progress of Y2K in mission critical and non-mission critical systems. Provide the DoD CIO and Component CIOs with the information they need to manage the Y2K initiative. Report to OMB on progress.

Objective 2.3 - Modernize and Integrate the Defense Information Infrastructure, Evolving It to the Global Information Grid

Strategy 2.3.1 - *Improve base-level infrastructure*. DoD's base level communications and computing infrastructure and data storage environment needs to be reengineered and upgraded. Inconsistencies in technical and management procedures and capabilities complicate IT change planning and implementation. A major effort will be required to put in place a consistent management structure and modernized IT able to deliver quality support.

Strategy 2.3.2 - *Integrate and enhance communications.* DoD communications have been significantly consolidated and enhanced for greater bandwidth, interoperability, and the addition of value-added services. However, the capacity of tactical links needs to be upgraded. Tactical communications must be digitized and capable of transferring multi-media information such as maps and images to warriors. Networks must be seamlessly integrated and managed across all levels (e.g., national, theater, tactical), and interfaces established with allies, coalition partners, and other government agencies.

Strategy 2.3.3 - *Continue DoD-wide applications implementation.* As DoD-wide applications (formerly referred to as migration systems) align applications support with DoD functions and processes, future IT investments should be linked directly to process improvements. DoD-wide applications must have plans to achieve acceptable levels of Joint Technical Architecture/Common Operating Environment (JTA/COE) compliance by 2002 or earlier. Continued emphasis must be placed on implementing applications to support reengineered processes that achieve mission and functional goals and measures of performance. COTS software should be used to the maximum extent possible. Information support providers, in house and contractors, must maintain a program of continual improvement keyed to user requirements, software best practices, and the software capability maturity models.

Strategy 2.3.4 - *Expedite shared data environment implementation*. Sharing data is key to interoperability

and quality data. Requirements are exploding for reliable, secure, efficient shared information repositories to support DoD-wide applications data and world wide web (WWW) information. Core mission critical data items must be logically organized and shared under the control of data "stewards" who are responsible for their quality and use. The target is an accessible set of DoD-wide repositories with information required to support DoD operations. Private facilities and sources should be assessed when considering alternatives.

Strategy 2.3.5 - ***Expedite implementation of common standards.*** The JTA/COE provides the standards and interface environment for interoperability and a transparent technical infrastructure that supports all applications. Wide implementation will reduce planning time for applications and enable their timely, incremental implementation in a "plug and play" environment. Infrastructure elements and applications should be JTA/COE compliant at appropriate levels by the year 2002 or earlier.

Strategy 2.3.6 - ***Reduce duplication and inefficiencies in the DII by evolving to a GIG***. DoD's communications and computing infrastructure needs to fully utilize existing assets. A major effort will be required to identify duplication, overlap and opportunities for joint use of infrastructure assets. The GIG will provide the "information fabric" that brings the notion of Information Superiority into reality, enabling the operational concepts of *JV2010*. GIG policies, plans and programs will embody the constructs that will create the computing model shift to information centric operations/warfare. GIG provides the means to structure the future of the Department's computing resources to achieve the reality of information superiority. At the core of GIG is the recognition of the pervasiveness and durability of distributed computing across the DoD. A networked mid-tier architecture will define the core of the GIG with the tenets of enterprise management, economies of scale, and information assurance governing its evolution.

Objective 2.4 - Introduce New Paradigms

Strategy 2.4.1 - ***Rapidly insert advanced technology to support the mission***. Technology is changing faster than the infrastructure can adapt. New methods are needed to gracefully introduce new technologies incrementally with manageable risk rather than requiring lengthy contracting and development efforts. Current approaches such as the JBC, ACTDs, AWEs, Joint Warfare Interoperability Demonstrations (JWIDs), Automated Information Technology Services (AITS), and the Joint Operational Leveraging of C4 Technology initiative must be integrated, expanded, and fully exploited to meet this challenge. Distributed, Internet environments must be used to assess, test, integrate, and acquire new IT capabilities and COTS products. The target is a systematic management structure and methodology that "pipelines" new technologies linked to evolving mission needs and smoothly supplies these capabilities to the field.

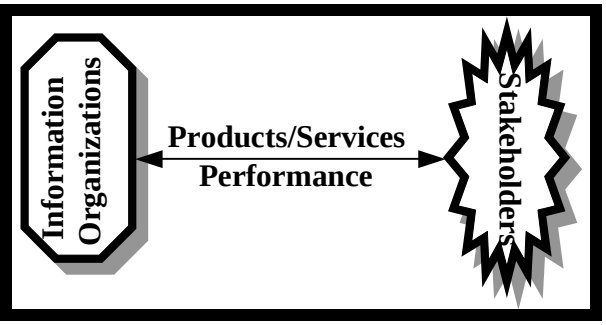
Strategy 2.4.2. ***Move to an information dissemination management (IDM) concept that implements an integrated approach to providing capabilities for improved awareness, access and delivery of information across the full spectrum of operations.*** Numerous initiatives are addressing IDM on an individual basis. A critical part of accomplishing the IM mission as set forth in this document is implementing IDM in a thoroughly integrated fashion. Therefore, IDM supporting the Global Broadcast Service (GBS) program will be used as a baseline with the expanded IDM effort led by USACOM used to guide all future IDM development. All Components will ensure their IDM related activities are integrated with and are compatible with the current IDM effort.

Strategy 2.4.3 – ***Facilitate the creation, capture, sharing and management of implicit and tacit organizational knowledge. Identify, centralize, and organize access to the numerous knowledge sources available and critical to the enterprise.*** Information technology and information services are essential but insufficient to achieve information superiority alone. Knowledge management offers the potential to significantly leverage the value of our information technology investments. The implementation of knowledge management methods and tools will facilitate collaborative knowledge creation and sharing and will, in turn, optimize the effectiveness of strategic and tactical decisions. The target is an agile, responsive, learning organization in which knowledge needed to provide critical mission support is available where and when needed.

Objective 2.5 - Improve IT Management Tools
Strategy 2.5.1 - ***Model and simulate the integrated information infrastructure***. A simulation model of the DII is needed to address cost, capability and performance over time for all infrastructure elements (e.g., communications, processing, data), and links to the mission. Existing models of DII segments and the DII Master Plan elements provide a starting point. The target is to provide comprehensive insight allowing CIOs and other decision makers to systematically evaluate personnel, service, cost/performance, acquisition, and operational issues and impacts.
Strategy 2.5.2 - ***Integrate information access and management methods for all media and types of information***. The user needs automated, streamlined methods to routinely and reliably access information. A common semantics, syntax, and procedures set would include electronic directories, such as the Government Information Locator Service (GILS), Defense Data Dictionary System (DDDS), Defense Messaging System (DMS) and directory and search methodologies employed by WWW information providers. Additionally, the Network Warfare Simulation (NETWARS) is under development and will be available beginning in CY99 to model key elements of the DII and to address these issues. The target is for on-line data dictionaries to be a primary source for DoD user assistance when accessing information (e.g., WWW documents).
Strategy 2.5.3 - ***Implement IT Total Asset Visibility (ITTAV) universally***. Total Asset Visibility is a Defense-wide initiative. The ITTAV concept can be used to manage IT "objects" like hardware, software, and data for the user throughout their life-cycle. ITTAV "tracking" includes tracking the status of user orders for IT objects, maintaining accurate inventory records, automatically ordering upgrades, and managing asset reuse and removal. The target is a WWW based repository that can be accessed by developers and users to determine availability, reliability, maintainability, etc., for any information or IT asset affecting their service.

GOAL 3

Reform IT management processes to increase efficiency and mission contribution



Description: As resources decline, information and information technology must be managed as a strategic resource, from a DoD-wide perspective. DoD must base information and information technology decisions on their contribution to the effectiveness and efficiency of military missions and supporting business functions. It is important to manage IT resources and align strategies and programs with Defense-wide, functional, and organizational goals and measures. Portfolios of IT investments must be linked to mission goals, strategies, and architectures, using various assessment and analysis tools. Strengthened Joint and Defense-wide processes are needed to plan, program, and budget IT to meet *JV2010* objectives, the *QDR* strategies, and Defense Reform Initiatives. Measures of performance for IT must be managed in the context of functional and organizational measures of performance to plan and assess IT's contribution to the mission. Information management, itself a business function, must employ best business practices to continuously improve customer/user support, reduce infrastructure costs, and apply the best available information technology.

Objective 3.1 - Institutionalize CCA Provisions

Strategy 3.1.1 - *Institutionalize IT strategic planning process.* This IM Strategic Plan will guide all DoD IT activities. DoD Component IM strategic plans have been instituted to proactively lead the linkage of IT to the mission starting with joint mission assessments and analyses. The linkage of the DoD and Component Plans must be strengthened in the near-term. Also, all IM strategic plans need to be better linked with the *QDR*, the *JV2010* Implementation Plan and process, and functional strategic plans.

Strategy 3.1.2 - *Make better, quicker outsourcing decisions*. Guidelines and criteria for systematically making outsourcing, privatization, in-house or partnering decisions are needed at all levels. Policy and procedures are needed to address issues such as IT outsourcing and privatization scope and context definitions, expectations and targets, elements of acceptable business case analyses, and use of these in oversight and resource allocation processes. Barriers, such as A-76 and lengthy cost studies, should be reexamined. Outsourcing and reengineering must be integrated within an overall IM process.

Strategy 3.1.3 - *Align IT investment decisions to support improved mission processes.* To support strategic plans and improved processes, IT alternatives must consider mission impacts (e.g., return on- nvestment) at the DoD-wide, functional, and organizational levels. DoD and Component IT investment criteria must be applied to develop IT portfolios for functions and organizations within the context of an overarching DoD IT portfolio managed by the DoD CIO and CIO Council.

Strategy 3.1.4 - *Improve acquisition processes.* Streamlined acquisition regulations and oversight processes can reduce acquisition overhead and lead time. Acquisition reforms should be fully implemented at all levels. Improved acquisition initiatives must fully integrate the efforts of the Joint C2 Integration and Interoperability Group (JC2I2G), the CINC Interoperability Program Offices (CIPOs), the Joint Forces Program Office (JFPO), the Joint Forces Command (JFC), and the Joint Staff to establish a joint Command, Control and Communication (C3) integrated system development process that emphasizes "joint first". Promising concepts and technologies from research experiments, pilot projects, and operational demonstrations must be moved through the acquisition process smoothly and efficiently. New paradigms of acquisition must be exploited that expedite the use of COTS (e.g., the Federal

Acquisition Regulation (FAR) Section 12, new testing rules for COTS), exploit commonalities (e.g., product lines), and provide insight into front-end processes (e.g., ACTDs) and other initiatives (e.g., Global Combat Support System (GCSS)). Selection, control, and evaluation of IT portfolios provide better links to the mission and base for improved management of individual systems and initiatives.

Strategy 3.1.5 - *Institute the customer/user focus*. Tools and policy will help activities systematically introduce and maintain customer awareness and compare their performance with peers. In industry, customer focus is routinely practiced and supports continuous improvement of processes, practices, and people. Routine use of customer surveys by IT organizations to measure satisfaction at all levels is a key approach (see Strategy 1.2.3).

Objective 3.2 - Institute Fundamental IT Management Reform Efforts

Strategy 3.2.1 - *Improve IT processes*. A comprehensive reengineering of IT processes themselves will serve to identify the optimum collection of information needed for efficient IT management. OSD, DISA, Army, Marine Corps and other existing models provide substantive baselines. Experience in the IT community can be exported to produce cost/performance gains and cross-functional optimization in other areas. This strategy envisions a comprehensive, time-phased plan for assessing and improving all IT processes, including strategic planning, policy and policy enforcement, requirements generation, programming and budgeting, acquisition, and operations.

Strategy 3.2.2 - *Establish uniform organizational measures and assessment processes*. Performance measures linked to mission need to be embedded systematically at all levels of DoD including local activities and IT staffs. While the focus is on organizational improvement, both Capability Maturity Models (CMM) and Baldrige criteria, for example, provide quantitative assessment methods that can be used as performance indicators.

Strategy 3.2.3 - *Improve methods and tools*. Tools have been provided to assist activities performing BPR, benchmarking, Total Quality Management (TQM), architectures and other improvement activities. These and other tools must be integrated into the actual life-cycle, so end-users, managers and developers can apply them easily, routinely, and incrementally, and also share results with others. Expansion is needed to make the capabilities available via WWW and useful for integrating with other DoD systems, including regular reporting.

Objective 3.3 – Promote the Development of an ITM Knowledge-Based Workforce Within DoD

Strategy 3.3.1 - *Provide training and educational opportunities*. Ensure that IM processes, policies and innovations are supported by appropriate training, professional development, and rewards for the work force of the DoD.

Strategy 3.3.2 - *Effectively utilize existing personnel processes, collaborate with other organizations (e.g., OPM) to create new policies, and implement a multi-faceted approach to acquiring, retaining, and maintaining highly skilled personnel in the IM/IT fields*. Use the recruitment process to acquire skilled personnel based on CCA core competencies. Use tools such as the performance evaluation process to assess employee performance to determine required training in areas of deficiency.

Strategy 3.3.3 – *Use organization and individual assessment tools to determine skill requirements.* Such tools can consist of surveys, studies, self-assessment and organization assessment tools (automated and non-automated models).

Objective 3.4 – Provide the IM/IT Support Required to Ensure Individuals with Disabilities Have Equal Access to the Information Environments and Opportunities in DoD

Strategy 3.4.1 – *Execute the Computer/Electronic Accommodations Program (CAP)*. Provide the hardware, software, and assistive technologies and services to make DoD work environments and

activities more accessible to individuals with visual, hearing, dexterity, and cognitive impairments.

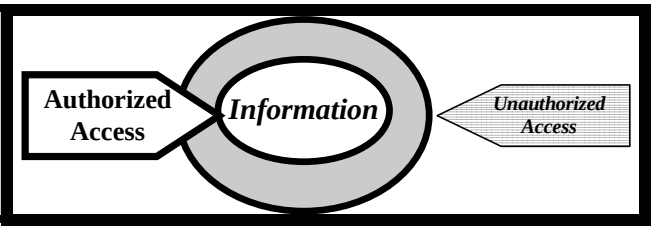
Objective 3.5 – Integrate DoD IT Activities

Strategy 3.5.1 – ***Provide tailored IM guidance for all missions and domains*****.** Ensure that IM processes, policies and innovations are appropriate for different mission and technical domains, including all NSS.

Strategy 3.5.2 – ***Identify relationships between IT activities in different domains*****.** Identify the relationships between IT applied in different domains to ensure that overarching objectives such as interoperability, information security, and efficiency are met; and mission threads, such as sensor-to-shooter, are effective. Dependencies such as those between IT activities in support missions (e.g., procurement, personnel) and the common infrastructure will be described and strategies for managing them established. Interoperable IT is integral to the effectiveness of our weapon systems.

GOAL 4

Ensure DoD's vital information resources are secure and protected



Description: The capability of DoD to carry out its mission from peacetime through conflict is highly dependent upon the GIG's interconnected set of information systems and networks derived from the DII and the expanding national and global infrastructure. In today's environment of sophisticated weaponry and rapid global force projection requirements, the ability to provide timely accurate information is vital to all aspects of DoD operations. Indeed, *Information Superiority* is at the very foundation of our vision of modern warfare, and Information Assurance (IA) is essential to achieve and maintain information superiority. IA is integral to *JV2010* and the ability to integrate intelligence, command and control, and battlefield awareness functions into joint and combined operations. IA is an essential element to implementing protection of critical national infrastructures mandated by the Presidential Decision Directive – 63, Critical Infrastructure Protection.

This view emphasizes the importance of IA to the Department's warfighting capability and recognizes the need to integrate IA into all facets of military operations. Such integration involves more than simply acquiring IA technology. It requires improving the awareness of individuals throughout the Department of the criticality of information operations and the role of IA in support of operational missions. Most importantly, it requires a clear operational understanding of the risks and impacts of an inadequate IA posture on defense missions. This perspective will require a significant cultural change in the approach to IA across the Department, one that recognizes IA as a warfighting concern and ranks it appropriately in Departmental attention and budgetary tradeoffs with other warfighting capabilities. Attaining increasingly effective, yet affordable, IA capabilities requires operational attention and a continuous improvement process that incorporates assessments of both risk and return on investment.

A robust IA program requires:

- concept of operations;
- continuous monitoring and assessment of threats, vulnerabilities, and readiness posture;
- appropriate architecture, technology, tools, and material;
- sufficient numbers of adequately educated and well-trained personnel;
- effective operational policies and doctrine;
- appropriate management and oversight; and
- the ability to quickly and efficiently implement agency-wide security measures and countermeasures to limit damage when threatened.

The Department's IA program includes specific goals and a strategy that guides the Department's activities and ensure that the vision of information superiority is achieved. The goals focus on protecting mission critical information, whether classified or sensitive but unclassified, using risk management techniques; taking advantage of global, national and defense information infrastructures while at the same time supporting security requirements at multiple assurance levels; furnishing robust and reconstitutable systems when required; and cultivating a cadre of information assurance professionals.

The underlying strategy to achieve these is process oriented and based on the principles of risk management, continuous improvement, and performance-based investment. It reflects:

- the strong link of information assurance to operational readiness;

- the need for a Defense-wide IA architecture;
- the need for continuous monitoring and reporting of the Department's IA posture;
- the use of the DoD CIO organization and management processes to address information assurance;
- a Department-wide IA program that provides the planning, coordination, integration, and oversight of the Department's IA resources and investments; and
- an awareness on the part of all members of the organization of the distinction between information that is operationally sensitive and information that can be made available to the public.

This approach must also address the vulnerabilities of the information infrastructure to physical as well as cyber attack. The disruption, failure or destruction of equipment or services (e.g., power, cooling, UPS, telecommunications) that support the information infrastructure have the potential to disrupt critical services just as much as cyber intrusion.

The Department's IA improvement efforts are guided by the following objectives and strategies:

Objective 4.1 – Make IA an Integral Part of DoD Mission Readiness Criteria

Strategy 4.1.1 - ***Designate all GIG functions as either mission critical, mission essential, or mission support***. DoD defense infrastructure owners (e.g., command and control, logistics and transportation, health affairs, intelligence, personnel, financial services), in coordination with the Joint Staff and the Critical Asset Assurance Program, shall identify those mission functions and information system elements of their infrastructures which perform mission critical, mission essential, or mission support functions.

Strategy 4.1.2 - ***Provide information assurance levels consistent with the Department's mission critical, mission essential, and mission support requirements for all networks of the DoD Components of the GIG***. Detailed assurance criteria for each level and interconnection between levels will be developed and specified.

Strategy 4.1.3 - ***Integrate IA readiness standards and metrics into the DoD readiness reporting process.*** Department IA policy must address the accountability aspects of IA. It must drive the availability of resources required by operational commanders and others accountable for their, and thus the Department's IA posture.

Objective 4.2 – Enhance DoD Personnel IA Awareness and Capabilities

Strategy 4.2.1 – ***Train and certify DoD network managers, operators, systems administrators, and all other personnel involved in the operation and management of the GIG and its component systems.*** Training and certification must extend into the contractor community supporting DoD.

Strategy 4.2.2 – ***Review and create (as needed) military and civilian career fields to ensure that they reflect adequate recognition of network information assurance skills and capabilities. New career fields shall be established as necessary.*** Career field designation is essential to establishing ascension paths for the military and civilian disciplines critical to ensuring efficient secure operation of the GIG.

Objective 4.3 – Enhance DoD IA Operational Capabilities

Strategy 4.3.1 - ***Protect the GIG with a defined and controlled perimeter.*** While DoD depends upon unclassified connections to the Internet to accomplish unclassified basic support functions and to provide access to open source information, these connections will be controlled and capable of being monitored. Interconnection of all classified systems with any other system will be accomplished by high assurance means. Authentication will be broadly employed.

Strategy 4.3.2 - ***Protect the GIG with an integrated attack sensing and response management capability***. As part of the integrated capability, all DoD Components of the GIG and all access points into the GIG will have intrusion detection capabilities.

Strategy 4.3.3 - ***All DoD Components of the GIG will adhere to established IA architecture, connection standards and procedures.*** All GIG elements will provide the required levels of security configuration management, employ methods to detect unauthorized activity and malicious code, and have adequate provisions for continuity of operations and rapid reconstitution.

Strategy 4.3.4 - ***Implement "Defense in Depth" concepts across the GIG.*** This concept will be applied to each operating assurance level and shall be applied in accordance with DoD criteria, including existing protective measures traditionally used to safeguard national security information. This strategy will consist of the following:

- Hardened network infrastructure.
- Protected host secure operating systems.
- Protected enclave boundaries.
- User/Application layer security services, including non-repudiation, signature, integrity, and confidentiality.
- Employment of strong identification and authentication (I&A) services.
- Use of a common, integrated DoD Public Key Infrastructure (PKI) to enable security services at multiple levels of assurance.
- IA situational awareness based on both network and host monitoring to formulate and support an attack sensing and response management capability.
- Approved high assurance devices and configurations for all interconnections among mission sensitivity levels.

Objective 4.4 – Establish an Integrated DoD Security Management Infrastructure (SMI)

Strategy 4.4.1 - ***Integrate a broad spectrum of network services (e.g., audit, intrusion detection, operational network monitoring and control) into the DoD SMI.*** Confidence in the secure operation of the GIG must be grounded in a real-time understanding of network-wide activities. Further, the ability to identify when network users have gained access to unauthorized areas or information or to be able to attribute specific network activity to specific users of the network is an important factor in dealing with the insider threat.

Strategy 4.4.2 - ***Implement the DoD PKI consistent with the May 6, 1999 policy memorandum, DoD PKI Roadmap, DoD PKI Implementation Plan, and the DoD PKI Certificate Policy.***

V. Implementation

The DoD IM Strategic Plan is a key part of an end-to-end strategic planning process designed to guide DoD Components in performing their IM strategic planning and implementation activities. OSD PSAs and the Joint Staff formulate their guidance for improving mission performance within each functional area and activity. Components develop their visions and strategic plans to accomplish their assigned missions and functions. The DoD IM Strategic Plan integrates IT management requirements from all functional areas and missions into crosscutting IM strategies to guide the Department's overall IM efforts. DoD Components use this guidance to prepare their IM plans and programs in support of their unique missions and to implement DoD-wide IM strategies

A. IM Strategic Planning Process

This section describes the IM strategic planning cycle. While this cycle is aligned with the PPBS, its influence extends beyond the formal planning, programming, and budgeting system into all information related activities. The primary purpose is to establish an IT management structure and process to improve IT support to the mission and successfully defend IT investments by demonstrating mission improvement. The CCA requires that an annual report be submitted with each budget showing actual results based on a strategic plan.

The IM strategic planning process includes development of both DoD and DoD Component strategic plans and the development of performance measures for assessment:

DoD Component Strategic Planning

Each DoD Component will maintain a DoD Component IM strategic plan consistent with the DoD IM Strategic Plan. DoD Component strategic plans will inherit the DoD goals and strategies and identify supporting initiatives. Additional sections may be added to identify performance gaps and specify additional goals, objectives, and supporting strategies. Actions to support formal goals and strategies can expect review and support from the DoD CIO during PPBS processes. DoD Component strategic plans will include their IT investment criteria and portfolio decision process.

Performance and Assessment

Strategic goals and strategies will be governed by formal performance measures as a routine management practice. DoD Component strategic plans will show how they support and contribute to the achievement of DoD-wide measures and targets and make performance information available. The annual report to the CIO council will report the actual performance results for their review. Appendix C describes the IT Performance Measurement Strategy and Implementation Program. As for the goals, objectives and strategies in this plan, much effort has been expended to develop performance measures, including convening an in-process review team (IPT), with little success. The importance of measuring our progress necessitates that further work be initiated to develop and implement performance measures for this plan.

The strategic planning and annual report cycle is keyed to CIO Council meetings and linked with DoD Component planning processes and OSD PPBS schedules. Actions include approving the DoD IM Strategic Plan, implementing near-term actions, reviewing planning and resourcing problems and opportunities, measuring performance and developing and approving annual report(s). Review for the annual report will be accomplished concurrent with strategic plan updates including performance and near-term action appendices.

Strategic Plan Interaction with PPBS

The DoD IM strategic plan can be an important contributor to the PPBS process and products. The top-level goals and strategies provide a common, coordinated basis for input to the DPG and to other Defense planning and detailed guidance for DoD Components.

DoD Component CIOs have a critical role in ensuring DoD IM goals and strategies are supported in DoD Component plans and in program and budget inputs. The guidance in the DoD IM Strategic Plan will be a common basis for developing DoD Component IM strategic plans. The combination of OSD and DoD Component plans will support DoD Component investment decision making during their program build processes and justify programs at the DoD level.

The IM Strategic Plan also is a basis for identifying issues for OSD program review. The adequacy of resources programmed to support DoD IM strategies and measures of performance will be assessed. Approved POMs make adjustments at the OSD level in the Future Year Defense Program (FYDP) submitted to OMB and Congress. In addition, significant strategic plan issues may necessitate "out-of-cycle" Program Budget Decisions (PBDs) and adjustments to the current budget year.

Appendix B provides a more detailed description of the interaction of the IM strategic planning process with the PPBS.

B. Near Term Actions – The DoD CIO Action Plan

The DoD CIO and Deputy CIO held an offsite working conference to provide a rapid, sound solution to the Department's need to do the following:

- Assess and focus on the most critical issues in defense information technology management today.
- Broadly and quickly communicate to the ITM community, the highest priorities of the DoD CIO.
- Effectively demonstrate to OMB and Congress that the Department vigorously supports the CCA.
- Energize the ITM community to actively participate in the Department's overall mission needs.
- Collectively produce a realistic ITM action plan to give the Department immediate direction and specific initiatives for the next 12-18 months.

More than 100 participants, representing 20 organizations, addressed the CIO's 4 key areas and the primary guiding principles:

- Y2K – Move beyond reactive mode.
- Network Enterprise – A physical and logical global network is overdue.
- Process Change – Critical if we are to optimize $10-$40 billion in IT funding.
- CIO Governance – Information is power and requires participatory governance to harness.

From discussions and consultations with the DoD Deputy CIO, Service CIOs, and Joint Staff, the group drafted an action plan. It is divided into 14 sub-areas with initiatives, actions, and resources. Major milestones are set for 1 month, 3 month, 6 month, and 1 year windows, and beyond. The action plan is a "living" document that depends on the iterative process for soundness, support, and actualization. During the course of its "life span", it is expected that particular details such as specific actions, deliverables, and due dates will change because of

unforeseen circumstances or circumstances beyond our control. However, the overall intent and spirit of the plan as embodied in the goals and initiatives will remain fairly constant to serve as pointers, guides, and priorities with which to direct our IM efforts in the coming year.

This off-site identified initiatives in several areas to include:

Year 2000
Network Enterprise
- Information Infrastructure and Security
- Software Licensing
- Standards

Process Reengineering
- Personnel
- Finance
- Mission Critical
- Logistics
- Electronic Commerce

CIO Governance
- IT Governance Process
- Policy
- Strategic Planning
- Performance Assessment
- Education and Training

The detailed explanation of each of the initiatives, deliverables and timeframes is provided in the DoD CIO Action Plan.

Appendix A - Guiding Principles

This appendix captures essential elements of the CCA, DoD Directives, presidential quality award management principles, and the National Defense Performance Review objectives. They identify general management improvement tenets and initiatives that impact formulation of IM goals and objectives.

Strategic Planning Guidelines

1. ***Improve defense processes.*** Employ business reengineering practices, methodologies and tools to develop or refine processes before system automation is undertaken. New business methods and procedures are proven and validated in pilot projects before organization-wide implementation. Information technology services are engineered to optimize process outputs (products and services) and outcomes (expectations and knowledge).
2. ***Take a user/customer focus.*** Information will be managed to: improve understanding; effectively provide user services; support informed choices by providers and beneficiaries; and recognize best value. Quality, interoperability and timeliness should be defined in terms of process and not the succession of interfaces. The warfighter knows the job to be performed and information needed. IM service providers must be immersed in the mission and the user environments to be able to communicate clearly the options available and to anticipate future needs for long lead-time items.
3. ***Ensure information is secure and available to authorized users.*** Information must be protected from attack and misuse, while at the same time being easily available to users who need it to perform their tasks. Our reliance on information must not be turned against us. IT capabilities must be sufficiently resilient, redundant and fail-safe to ensure continuity of operations under traditional and emerging threats. Catastrophic failures in our global information grid could present our adversaries with an "information Achilles heel."
4. ***Promote accountability.*** Programs and resources will be aligned to joint requirements and priorities and implemented through strong cost and performance linkages with the PPBS processes at all levels. Accountability for product and service cost and performance goal accomplishment must be at each level, replacing hierarchical models.
5. ***Integrate commercial capabilities***. Capitalizing on commercial products and services can recognize tremendous life cycle savings. Changing processes to accommodate "off-the-shelf" products and services need to be considered and balanced with DoD development, deployment, training and support costs. Critical skills, knowledge, and capabilities must be mobilized to support defense missions in military, civilian, and/or industrial organizations. Outsourcing functions and employing COTS products and services free resources for application to unique DoD missions.
6. ***Foster learning, collaboration and empowerment.*** Our processes must motivate and reward our military and civilian personnel and industry partners to act from a joint, Defense-wide perspective to realize our shared vision for the future. We must become a learning organization, work as a team, and empower people to achieve excellence in meeting future defense challenges. Self-assessment instruments articulate policy and doctrine at the job/organization level, eliciting understanding and accountability, replacing extraneous oversight and reporting.
7. ***Achieve the required degree of interoperability***. Interoperability must be measured on an end-to-end basis. End users must understand and use the information presented. Further, we must be able to share and use knowledge and capabilities jointly and with our allies and coalition partners to the degree necessary to meet mission needs. Our capabilities must transcend a single language and ensure a common understanding as the basis for working and winning as a joint and combined force.

8. ***Exploit models and architectures.*** Process and data models and various architectures define information requirements and guide support strategies over the long-term (5-10 years). The IT initiatives must use approved architectures and formal methods available to evolve them through use of change requests. We must replace hardware and software based management with doctrinally-driven operational requirements, captured in architectures, translated into capabilities that are responsive to information needs and changing missions and doctrine.
9. ***Demand adaptable, innovative, incremental, and modular approaches and solutions.*** Capabilities must be tailorable, scaleable, and configurable, so that the right "package" of capabilities can be assembled, integrated, and applied to each unique contingency and crisis. In the field, capabilities must rapidly adapt to the full range of operational conditions, new situations and technologies without complete redesign. Our processes and practices must become more innovative, while maintaining a focus on a shared vision. Modernization and contracting efforts will employ incremental, modular strategies to reduce risk and increase responsiveness to user requirements and transparently introduce new technologies. These must be accomplished in a compressed time frame to minimize the cost of development and achieve early realization of benefits.
10. ***Promote efficiency and reduce duplications.*** IT solutions should incorporate the concepts of reuse, dual use, bundling, and consolidation whenever possible.

Implementation Planning Guidelines

1. ***Build on current programs and capabilities***. The seeds for achieving the strategic goals are now emerging. These should be fully exploited wherever possible. Examples include *JV2010* and other strategic plans, GIG, DII COE, Global Command and Control System (GCCS), GCSS, C4ISR Report and Mission Area Assessment, process improvement projects, TQM efforts, GPRA pilots, modeling and simulation, DoD-wide applications, and the IA Program.
2. ***Maintain current program and operations assessments***. Linking projects and programs to strategies and measures provides a basis for determining funding levels and go/no go decisions.
3. ***Move to product/service/performance based structures***. Management techniques emerging from GPRA pilots and CCA policies describe our organizations and support structures in terms of processes, outcomes, products and services, and customer expectations. Customer decision cycles drive management decisions, and efficiencies are determined by comparing unit performance with the best government or industry benchmarks. Architectures, interoperability, and acquisitions are measured in terms of end-to-end product/service rather than infrastructure component performance.
4. ***Help people adapt.*** Performance based organization concepts emphasize collaboration, teamwork, customers, and services/production. This is a major change for the DoD. Jobs are defined by tasks depending on a mix of knowledge and skills as much as organization position. Basic values such as identity, loyalty, security, and interpersonal relationships change and need to be reinterpreted. Education and training move to incremental and "just in time" strategies. These "cultural" transitions often dictate the pace of accomplishing the other objectives.
5. ***Promote senior management involvement***. Senior managers must understand, adopt and promote strategic objectives. Performance based organizations assume agility and change based on trust and openness to discover how organizations work together to provide end-to-end service to customers. Current systems reward building and maintaining stove-piped organizations that can stalemate innovation and destroy teamwork.
6. ***Couple mid-term and long-term goals with near-term actions***. Strategic plans must set longer term goals to guide and synchronize major efforts but also identify near-term actions, start transitions, and gain credibility.

Performance Guidelines

1. ***Link to Strategic Planning.*** Wherever possible, performance measures should be linked to strategic planning missions, visions, goals, objectives, or strategies. Strategic plans provide the context to define individual measures and interaction between measures.

2. ***Engage stakeholders***. Stakeholders are evident at each organizational level and can include: (1) customers and suppliers -- current and future, (2) employees and support contractors -- current and future, (3) higher order management (e.g., headquarters, OSD, OMB, Congress), (4) subordinate organizations seeking guidance (e.g., headquarters-field, OMB-OSD, OSD-Military Departments).

3. ***Empower the field***. Empowerment means making the factors for incentives and disincentives of actions and decisions visible to all parties, precluding the need for oversight. Performance measures are a key methodology. Strategies and tools must allow local managers to define and measure performance and results against stakeholder expectations.

4. ***Measure outcomes wherever possible***. Measures are typically categorized as input, output, and outcome. Input measures are relatively easy to quantify and capture, e.g., resources, requests, students, etc. Output measures can be quantified for organizations with formal product and service descriptions but difficult for those with more abstract mission statements. Outcome measures of the vision or stakeholder satisfaction with products and services are multi-dimensional and hard to identify and quantify. However complex, outcome measures are the most valuable for decision making.

5. ***Focus on achievement***. Measures are applied at many levels. A few, well chosen, outcome-oriented measures are better than multiple, potentially conflicting, sub-optimal measures. All efforts should be focused on one or more measures mutually arrived at in consultation with stakeholders.

6. ***Find trend indicators***. Indicators will be selected to measure progress towards a particular goal or target. The user should be able to graph value with respect to time for quality, quantity, etc. For complex environments, values will typically be represented as a "high, low, most likely" to represent the range of responses and preclude excessive description necessary to defend a single value. *Note that completion of an action is not a trend.*

7. ***Use widely accepted methods***. The Baldrige criteria and CMM are comprehensive, long-term, proven methodologies for improving organization effectiveness, including performance. They benefit from extensive discussion, application in a variety of environments, and frequent review and refreshment. Robust infrastructures of information, benchmarks, training, and experience are augmented by a culture of openness and sharing. Participation reduces personnel and financial investments and also lead-time. International Standards Organization (ISO)-9000 standards and various customer survey instruments are also available.

8. ***Make the "business case" for each measure***. Performance measurement procedures have matured over time. Initial efforts often created apparently useful measures that proved ineffective because the the processes for gathering and using performance information were inadequately defined, the cost of gathering information outweighed the benefits, and user responses to the measures detracted from achieving the goal. Practitioners have identified templates to ensure effective measures are defined. Common questions that must be addressed include: (1) What is the measure supposed to show? (2) Who measures and how? (3) Who uses and for what? (4) How could the measure be used to subvert or be misinterpreted (unintended consequences)? (5) How much will it cost to measure? (6) What is the estimated value to the user? (7) Are there any provisions such as tools and assistance that could help? and (8) Are there any critical factors that need to be considered?

Appendix B - DoD IM Strategic Plan Linkage with the PPBS

The DoD IM strategic planning process is the way the CIOs in DoD establish the Department's IM vision and plan for the future. The planning process ensures the IT vision is grounded in the Department's mission requirements. It is interfaced with other management processes to ensure the DoD IM Strategic Plan is executed through the right set of initiatives, programs and investments.

The IM strategic planning process will be institutionalized in DoD IT policy which will *bring IT strategic planning in line with the guidance in the CCA and other relevant laws*.

DoD Strategic Planning

The IM planning flow is highlighted in Figure 1 in the context of other strategic planning and links to programming. The President's National Security Strategy drives the formulation of the National Military Strategy (NMS) by the Joint Chiefs of Staff (JCS). *JV2010* articulates the Chairman's future concepts for joint military operations. The *QDR*, under the leadership of the Secretary, defines the goals and major strategies for the Department to move into the 21st century. It shows how the Department will exploit the RMA and the RBA. The *QDR* is the DoD Strategic Plan that responds to the GPRA of 1996. Under this capstone guidance, PSAs prepare functional strategic plans for their assigned areas of responsibility such as logistics, finance, health, and personnel. Components prepare visions and strategic plans to accomplish their organizations' missions and functions. The DoD IM Strategic Plan is aligned with DoD, functional, and Component visions/plans to ensure that DoD IT optimally supports the entire Defense mission. IM guidance is included in the DPG. Components prepare POM inputs which balance all guidance and requirements. OSD reviews POM inputs to ensure they satisfy DPG and other guidance such as the DoD IM Strategic Plan. The budgeting processes lead to an authorized defense program.

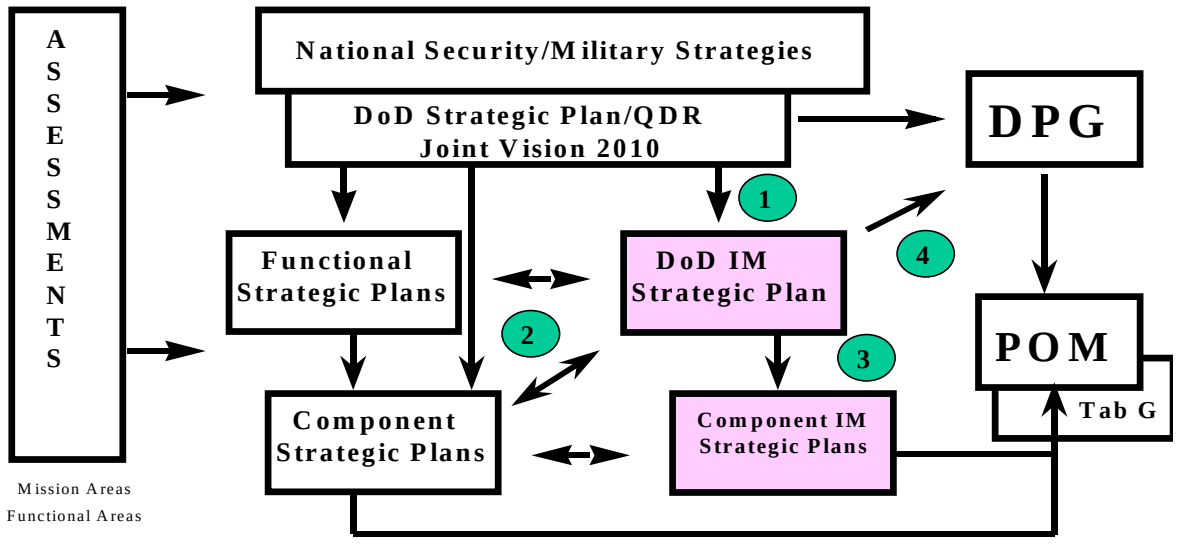


Figure 1. DoD IM Strategic Planning Flows and Links

As shown in the figure above, there are four key linkages (labeled 1-4) between the DoD IM Strategic Plan and:

1. The DoD Strategic Plan/*QDR* and *JV2010*
2. Functional and Component strategic plans
3. Component IM Strategic Plans, and
4. The DPG and the POM Tab G

Links 1 and 2 ensure the DoD IM Strategic Plan supports mission requirements. Link 3 leads to a consistent set of IM plans across the Department. Link 4 ensures that IM strategies are implemented in programs and investment portfolios.

Alignment of DoD IM Strategic Plan with the Mission

Developing and coordinating the DoD IM Strategic Plan is a challenge. The plan must support all the missions and functions of the Department and be aligned with corporate goals and strategies. All mission areas and organizations rely upon a common information infrastructure to communicate, collaborate, and work together as a team. Therefore, the plan must establish a Defense-wide IM roadmap based on common standards, uniform architectures, interoperable and integrated capabilities, and improved processes and practices. The IM community will work with its different customer communities to understand their missions and offer balanced strategic guidance that maximizes the value of IM across the Department. At the DoD level, the key is to integrate requirements across missions, assess options, and set priorities within constrained resource envelopes. Figure 2 shows the process for developing and maintaining the DoD IM Strategic Plan.

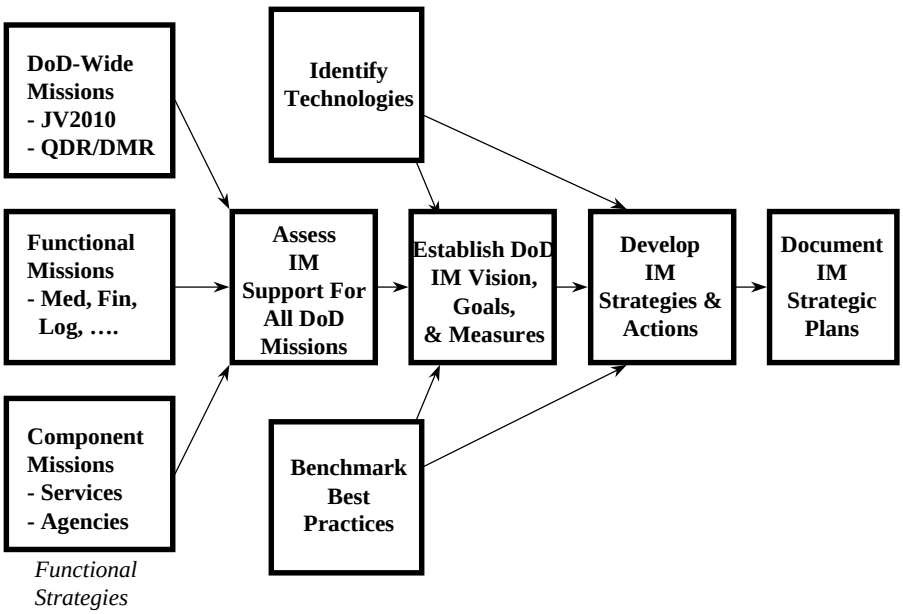


Figure 2. Process to Develop and Maintain the DoD IM Strategic Plan

Each functional community (e.g., warfighting, intelligence, mission support) assesses its processes and activities and develops strategies for improving performance and mission outcomes. The DoD CIO looks across the mission areas and organizational elements to provide a Defense-wide perspective for IT support. The DoD CIO develops the DoD IM vision, goals, objectives, and measures

of performance. To achieve the vision, the DoD CIO provides a set of strategies for implementation across the Department – a roadmap to the future.

The DoD IM Strategic Plan crosscuts all Defense activities. In order to ensure that the DoD IM Strategic Plan is aligned to the total Defense mission, the plan will be reviewed by key customers and stakeholders for its adequacy to support and enable all missions and functions. Issues arising from this review will be provided to the DoD CIO and the DoD CIO Council for resolution.

Aligning the DoD IM Strategic Plan with Component IM Strategic Plans

Component CIOs will prepare their IM strategic plans to satisfy Joint, Defense-wide, and unique requirements for IT support to their missions. The Components need to ensure that their IM plans are aligned to their functional strategic visions and plans and provide an IM vision for their subordinate (i.e., major) commands. Components inherit the vision, goals, objectives, and strategies from the DoD IM Strategic Plan. While Components may extend and expand the direction provided in the DoD IM Strategic Plan, the maximum degree of planning consistency is essential to ensuring that IT capabilities will be joint, interoperable, integrated within a DoD-wide system of systems architecture, and non-duplicative.

For each DoD strategy, Components will describe the initiatives, programs and projects (the "roadmap") that will accomplish or contribute to the Defense-wide IM strategy. The DoD CIO will assess these roadmaps for their adequacy in achieving the DoD IM Strategic Plan. For example, each Component will develop a strategy for complying with the Defense-wide plan to converge to a DII COE. These Component strategies need to be consistent to ensure that resulting systems are interoperable.

Conceptually, the DoD IM Strategic Plan and the Component IM strategic plans provide a *seamless, hierarchical planning structure* that drives programs and resources, and ultimately reaches down to field activities to achieve the Department's IM vision. Components will work closely with the DoD CIO staff to ensure that the DoD IM Strategic Plan is realistic, affordable, and supports Component missions. Experience in implementing strategies at the Component level will be used to improve the DoD Plan. This iterative cycle of implementation and feedback will result in a "top-to-bottom" defense IM planning structure that reflects changing circumstances and incorporates lessons-learned from actual experience.

Translating the IM Plan into Programs and Investment Portfolios

Specific guidance from the plan that needs to be emphasized will be incorporated in the DPG. To ensure the plan can be executed and achieve an integrated system of systems, the DoD CIO will formulate guidance for a DoD IT portfolio of investments. *Conceptually, the DoD IT portfolio consists of the aggregate of DoD-wide and Component portfolios.* OSD will establish guidance for:

- Functional AIS
- Infrastructure
- Related Technical Activities

Components will provide IT portfolios in the POM, in accordance with Tab G instructions. This uniform planning and programming structure will enable the DoD CIO and Component CIOs to gain insight into all IT initiatives and programs at all levels and ensure that they satisfy defense goals, meet investment criteria, are consistent, avoid unnecessary duplication, and share common resources within an overarching system of system architecture.

Planning Schedule

The IM strategic planning process is scheduled to mesh with the PPBS and other key events. In order to mesh with the PPBS, this plan will be updated every two years, with any necessary interim changes published as a supplemental release. The DoD CIO will develop the plan in collaboration with Component CIOs and other stakeholders in the fall. A plan will be issued in December for review by stakeholders and customers. The plan will also be a basis for the Components to conduct a dialog on Defense-wide IM strategies and reach consensus on a roadmap for DoD IM. The plan will be used to develop inputs to the DPG. Component CIOs will submit their approved IM strategic plans to the DoD CIO in July of the following year.

Appropriate guidance from the DoD IM Strategic Plan will also be included in the DPG. The DoD CIO will develop DoD portfolio guidance to supplement the IM Strategic Plan based on front-end assessments. Figure 3 shows the IM strategic planning cycle.

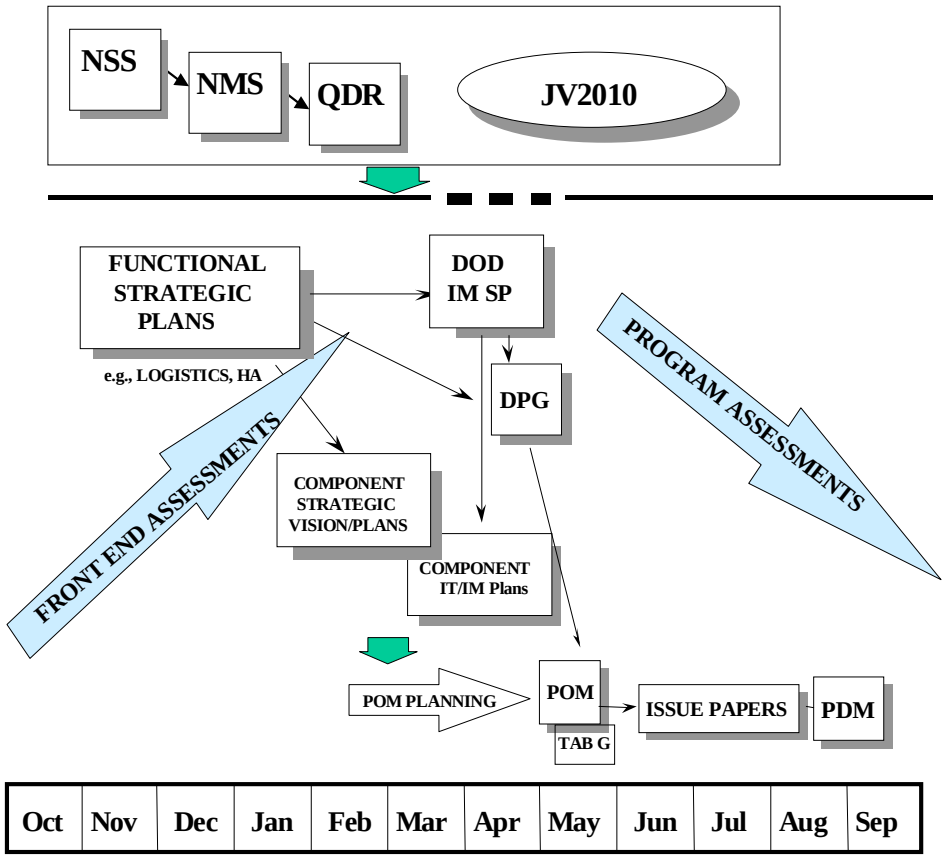


Figure 3. IM Planning Cycle

This schedule synchronizes the IM Plan with other strategic assessment processes such as *JV2010* Implementation and the JWCA. It provides guidance in time to influence the DPG.

Appendix C – IT Performance Measurement

Performance Measurement Strategy & Implementation Program

The Department continues to support the full institutionalization of performance measures for its IT investments.

Establishment of IT Acquisition and Investment Directorate

The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) has been significantly reorganized to more effectively measure DoD information technology performance within the context of functional mission outcomes. One result of this reorganization was the establishment of the IT Acquisition and Investment Directorate under the DoD, Deputy Chief Information Officer. This directorate is now responsible for promulgating performance measurement guidance, methods and tools, and experimental methodology, and incorporating performance measurement as the cornerstone to conducting IT investment portfolio oversight and CIO/CFO IT outcome-based POM and budget assessments.

DoD Performance and Results Based Management Pilot Program

The Department conducted a Chief Information Officer's Performance Measures Executive Pilot Program to evaluate the usefulness of the *Guide for Managing Information Technology as an Investment and Measuring Performance*, the Investment Baseline/Performance Agreement, and the CIOEXEC automated system. The overall objective of the pilot was the development of tools and procedures to strengthen DoD compliance with recent legislation, such as CCA and GPRA, and to evaluate tools for measuring mission performance and benefits. The pilot program, which concluded on September 30, 1998, examined the use of performance measures during the Control Phase of the IT investment process using actual data. The Defense Medical Logistics Standard System (DMLSS) program served as the pilot test case. The DMLSS program is at the forefront in applying best business practices such as business re-engineering and mission-related performance measurement. In addition, the program has sufficient cost, schedule, and historical performance data to enable a meaningful examination of the prototype.

The pilot test case found that the DoD *Guide for Managing IT as an Investment and Measuring Performance* is comprehensive and consistent with General Accounting Office (GAO) guidance. Further, it aligns the GAO guidance with the DoD acquisition process. The Information Performance/Baseline Agreement is a flexible, tailorable document that enables cost, schedule, and mission-performance information to be identified and tracked. The pilot recommended that the IP/BA be expanded in the area of tracking post-deployment mission performance. The pilot demonstrated that CIOEXEC can link information from the DoD Departmental level to the Component level, from the Component level to the functional level, and from the functional level to the program level. These views provide the CIO information needed for early problem identification and avoidance.

As an outgrowth of the DMLSS pilot, a DoD CIO Executive Advisory Board was established to take a broader look at the capital investment process. The Board examined the Health Affairs processes, identified best practices, and published its report on August 19, 1998. The Executive Advisory report concluded that Health Affairs (HA) has effective management and oversight structures that ensure extensive involvement by the functional community and the HA CIO. A key success factor is that HA has a consolidated Tri-Service (Army, Navy, Air Force) program that allows prioritization of investments across the entire Departmental enterprise. Continual program evaluation, monitoring, and problem resolution in HA results in a very effective investment program that reflects the priorities of the HA community.

The IT Acquisition and Investment Director is using the results of these efforts as a point of departure for developing policy and implementing procedures for measuring performance of IT programs throughout the Department.

Information Technology Investment Portfolio Oversight

The Department recognizes that its current IT management process has the following shortfalls: (1) minimal linkage between IT investments and functional direction/process changes; (2) individual systems narrowly focused on specific functions and organizations vice total mission; and (3) fragmented systems and infrastructure, resulting in a lack of fully integrated and interoperable capabilities. To correct these deficiencies, the IT Acquisition and Investment Directorate is developing an IT investment portfolio (ITIP) oversight approach that will: (1) provide the DoD CIO with better information to support management and investment decisions and fully implement IT performance measurement within the Department; (2) assist functional managers to effectively build and manage IT portfolios consistent with their strategic visions, goals, and measures of performance; and (3) assist Program Managers to effectively manage performance, cost, and schedule risks in the acquisition of IT that supports functional mission needs and strategic plans.

Building upon the work accomplished by the DoD Performance and Results Based Management Pilot Program, a Directorate team has developed a draft ITIP template. Over the next year, this template will be validated through a series of pilots, under the auspices of a DoD-wide Working-Level Integrated Product Team, with the eventual goal of adopting it for Departmental use.

Appendix D – List of Acronyms

ACC	Architecture Coordinating Council
ACTD	Advanced Concept Technology Demonstration
AIS	Automated Information System
AIT	Automated Information Technology
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
AWE	Advanced Warfighting Experiment
BPR	Business Process Reengineering
C2	Command and Control
C3	Command, Control and Communications
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAP	Computer/Electronic Accommodations Program
CCA	Clinger-Cohen Act of 1996
CFO	Chief Financial Officer
CIPO	CINC Interoperability Program Office
CINC	Commander in Chief
CIO	Chief Information Officer
CMM	Capability Maturity Model
COE	Common Operating Environment
COTS	Commercial-Off-the-Shelf
CRD	Capstone Requirements Document
DARPA	Defense Advanced Research Projects Agency
DDDS	Defense Data Dictionary System
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DMLSS	Defense Medical Logistics Standard System
DMS	Defense Messaging System
DoD	Department of Defense
DPG	Defense Planning Guidance
DRIR	*Defense Reform Initiative Report*
EB/EC	Electronic Business/Electronic Commerce
EBO	Electronic Business Operations
EOC	Enterprise Operation Center
FAR	Federal Acquisition Regulation
FYDP	Future Year Defense Program
GAO	General Accounting Office
GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIG	Global Information Grid
GILS	Government Information Locator Service
GPRA	Government Performance and Results Act of 1993
HA	Health Affairs
IA	Information Assurance
IDM	Information Dissemination Management
IM	Information Management
IPT	In-Process Review Team
IRM	Information Resources Management
ISO	International Standards Organization

ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
ITIP	Information Technology Investment Portfolio
ITM	Information Technology Management
ITTAV	Information Technology Total Asset Visibility
JBC	Joint Battle Center
JC2I2G	Joint Command and Control Integration and Interoperability Group
JCS	Joint Chiefs of Staff
JFC	Joint Forces Command
JFPO	Joint Forces Program Office
JTA/COE	Joint Technical Architecture/Common Operating Environment
JV2010	*Joint Vision 2010*
JWCA	Joint Warfighting Capabilities Assessment
JWID	Joint Warfare Interoperability Demonstration
M&S	Modeling and Simulation
NATO	North Atlantic Treaty Organization
NETWARS	Network Warfare Simulation
NMS	National Military Strategy
NPR	National Performance Review
NSS	National Security Systems
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
PBD	Program Budget Decision
PDM	Program Decision Memorandum
PKI	Public Key Infrastructure
POM	Program Objective Memorandum
PPBS	Planning, Programming, and Budgeting System
PRA	Paperwork Reduction Act
PSA	Principal Staff Assistant
QDR	*Quadrennial Defense Review*
RBA	Revolution in Business Affairs
RMA	Revolution in Military Affairs
RML	Revolution in Military Logistics
SMI	Security Management Infrastructure
TAFIM	Technical Architecture Framework for Information Management
TQM	Total Quality Management
UPS	Uninterrupted Power Source
USD(C)	Under Secretary of Defense for Comptroller
WWW	World Wide Web
Y2K	Year 2000

Appendix E - Glossary

Automated Information System (AIS): Computer hardware, computer software, telecommunications, information technology, personnel, and other resources that collect, record, process, store, communicate, retrieve, and display information. An AIS can include computer software only, computer hardware only, or a combination of the above.

Commercial-Off-the-Shelf (COTS): Refers to an item of hardware or software that has been produced by a contractor and is available for general purchase. Such items are at the unit level or higher. Such items must have been sold and delivered to government or commercial customers, must have passed customer's acceptance testing, and must be operating under the customer's control and within the user environment. Further, such items must have meaningful reliability, maintainability, and logistics historical data.

Common Operating Environment (COE): The DII COE establishes an integrated software infrastructure, which facilitates the migration and implementation of functional mission applications and integrated databases across information systems in the Defense Information Infrastructure. The DII COE provides architecture principles, guidelines, and methodologies that assist in the development of mission application software by capitalizing on a thorough, cohesive set of infrastructure support services. The DII COE specification is derived from the complete TAFIM.

Defense Information Infrastructure (DII): The web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of DoD users, across the range of military operations.

DoD Components: In this plan the term collectively refers to the Military Departments, the Defense Agencies, and the DoD Field Activities.

Electronic Business/Electronic Commerce: The interchange and processing of information via electronic techniques for accomplishing transactions based upon the application of commercial standards and practices. Further, an integral part of implementing EB/EC is the application of business process improvement or reengineering to streamline business processes prior to the incorporation of technologies facilitating the electronic exchange of business information.

Global Information Grid: The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

Information: Any communications or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Management: The planning, budgeting, manipulating, controlling of information throughout its life-cycle (e.g., creation or collection, processing, dissemination, use, storage, and disposition).

Information Resources: Information and related resources, such as personnel, equipment, funds, and information technology.

Information Resources Management: The process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources such as personnel, equipment, funds, and information technology.

Information Services: A discrete set of information activities typically provided on a reimbursable basis. These activities include analysis, acquisition, test, delivery, operation, or management of hardware, software, and communications systems.

Information Superiority: The ability to obtain and transmit information unimpeded to any destination as and when needed and to exploit or deny an adversary's ability to do so. This includes the ability to manage information throughout its life-cycle, i.e., to create, collect, process, disseminate, use, store and dispose of an unimpeded flow of information while exploiting or denying an adversary's ability to do the same.

Information Technology: (A) Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

(B) The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

(C) Notwithstanding subparagraphs (A) and (B), the term 'information technology' does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Infrastructure: Infrastructure is used with different contextual meanings. Infrastructure most generally relates to and has a hardware orientation but note that it is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. Again note that just citing standards for designing an architecture or infrastructure does not include functional and mission area requirements for performance. Performance requirement metrics must be an inherent part of an overall infrastructure to provide performance interoperability and compatibility. It identifies the top-level design of communications, processing, and operating system software. It describes the performance characteristics needed to meet database and application requirements. It provides a geographic distribution of components to locations. The infrastructure architecture is defined by the service provider for these capabilities. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs.

Joint Technical Architecture: The JTA identifies a common set of mandatory information technology standards and guidelines to be used in all new and upgraded C4I acquisitions across DoD.

Operational Architecture: A description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges.

Systems Architecture: Defines the physical connection, location, and identification of key nodes, circuits, networks, warfighting platforms, etc. and specifies system and component performance parameters. The systems architecture is constructed to satisfy operational architecture requirements per standards defined in the technical architecture. The systems architecture shows how multiple systems within a subject area link and interoperate, and may describe the internal construction or operations of particular systems within the architecture.

Technical Architecture: The technical architecture identifies the services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed.